ABSTRACT

Disclosed are systems and methods which examine information communication streams to identify and/or eliminate malicious code, while allowing the good code to pass unaffected. Embodiments operate to provide spam filtering, e.g., filtering of unsolicited and/or unwanted communications. Embodiments provide network based or inline devices that scan and scrub information communication in its traffic pattern. Embodiments are adapted to accommodate various information communication protocols, such as simple mail transfer protocol (SMTP), post office protocol (POP), hypertext transfer protocol (HTTP), Internet message access protocol (IMAP), file transfer protocol (FTP), domain name service (DNS), and/or the like, and/or routing protocols, such as hot standby router protocol (HSRP), border gateway protocol (BGP), open shortest path first (OSPF), enhanced interior gateway routing protocol (EIGRP), and/or the like.